CHAPTER 72

Configuring Logging

This chapter describes how to configure and manage logs for the adaptive security appliance and includes the following sections:

- Information About Logging, page 72-1
- Licensing Requirements for Logging, page 72-5
- Prerequisites for Logging, page 72-5
- Guidelines and Limitations, page 72-5
- Configuring Logging, page 72-6
- Configuration Examples for Logging, page 72-20
- Log Monitoring, page 72-19
- Feature History for Logging, page 72-20

Information About Logging

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. Cisco devices can send their log messages to a UNIX-style syslog service. A syslog service accepts messages and stores them in files, or prints them according to a simple configuration file. This form of logging is the best available for Cisco devices, because it can provide protected long-term storage for logs. Logs are useful both in routine troubleshooting and in incident handling.

The adaptive security appliance system logs provide you with information for monitoring and troubleshooting the adaptive security appliance. With the logging feature, you can do the following:

- Specify which syslog messages should be logged.
- Disable or change the severity level of a syslog message.
- Specify one or more locations where syslog messages should be sent, including an internal buffer, one or more syslog servers, ASDM, an SNMP management station, specified e-mail addresses, or to Telnet and SSH sessions.
- Configure and manage syslog messages in groups, such as by severity level or class of message.
- Specify whether or not a rate-limit is applied to syslog generation.
- Specify what happens to the contents of the internal log buffer when it becomes full: overwrite the buffer, send the buffer contents to an FTP server, or save the contents to internal flash memory.
- Filter syslog messages by locations, severity level, class, or a custom message list.

This section includes the following topics:

- Logging in Multiple Context Mode, page 72-2
- Analyzing Syslog Messages, page 72-2
- Syslog Message Format, page 72-3
- Severity Levels, page 72-3
- Filtering Syslog Messages, page 72-4
- Message Classes and Range of Syslog IDs, page 72-4
- Using Custom Message Lists, page 72-5

Logging in Multiple Context Mode

Each security context includes its own logging configuration and generates its own messages. If you log in to the system or admin context, and then change to another context, messages you view in your session are only those messages that are related to the current context.

Syslog messages that are generated in the system execution space, including failover messages, are viewed in the admin context along with messages generated in the admin context. You cannot configure logging or view any logging information in the system execution space.

You can configure the adaptive security appliance to include the context name with each message, which helps you differentiate context messages that are sent to a single syslog server. This feature also helps you to determine which messages are from the admin context and which are from the system; messages that originate in the system execution space use a device ID of **system**, and messages that originate in the admin context use the name of the admin context as the device ID.

Analyzing Syslog Messages

The following are some examples of the type of information you can obtain from a review of various syslog messages:

- Connections that are allowed by adaptive security appliance security policies. These messages help you spot holes that remain open in your security policies.
- Connections that are denied by adaptive security appliance security policies. These messages show what types of activity are being directed toward your secured inside network.
- Using the ACE deny rate logging feature shows attacks that are occurring against your adaptive security appliance.
- IDS activity messages can show attacks that have occurred.
- User authentication and command usage provide an audit trail of security policy changes.
- Bandwidth usage messages show each connection that was built and torn down, as well as the duration and traffic volume used.
- Protocol usage messages show the protocols and port numbers used for each connection.
- Address translation audit trail messages record NAT or PAT connections being built or torn down, which are useful if you receive a report of malicious activity coming from inside your network to the outside world.

Syslog Message Format

Syslog messages begin with a percent sign (%) and are structured as follows:

```
%ASA Level Message_number: Message_text
```

Field descriptions are as follows:

ASA	The syslog message facility code for messages that are generated by the adaptive security appliance. This value is always ASA.
Level	1 through 7. The level reflects the severity of the condition described by the syslog message—the lower the number, the more severe the condition. See Table 72-1 for more information.
Message_number	A unique six-digit number that identifies the syslog message.
Message_text	A text string that describes the condition. This portion of the syslog message sometimes includes IP addresses, port numbers, or usernames.

Severity Levels

Table 72-1 lists the syslog message severity levels. You can assign custom colors to each of the severity levels to make it easier to distinguish them in the ASDM log viewers. To configure syslog message color settings, either choose the **Tools > Preferences > Syslog** tab or, in the log viewer itself, click **Color Settings** in the toolbar.

Table 72-1 Syslog Message Severity Levels

Level Number	Severity Level	Description
0	**emergencies**	System is unusable.
1	**alert**	Immediate action is needed.
2	**critical**	Critical conditions.
3	**error**	Error conditions.
4	**warning**	Warning conditions.
5	**notification**	Normal but significant conditions.
6	**informational**	Informational messages only.
7	**debugging**	Debugging messages only.

Note The adaptive security appliance does not generate syslog messages with a severity level of zero (emergencies). This level is provided in the **logging** command for compatibility with the UNIX syslog feature but is not used by the adaptive security appliance.

Message Classes and Range of Syslog IDs

For a list of syslog message classes and the ranges of syslog message IDs that are associated with each class, see the *Cisco ASA 5500 Series System Log Messages*.

Filtering Syslog Messages

You can filter generated syslog messages so that only certain syslog messages are sent to a particular output destination. For example, you could configure the adaptive security appliance to send all syslog messages to one output destination and to send a subset of those syslog messages to a different output destination.

Specifically, you can configure the adaptive security appliance so that syslog messages are directed to an output destination according to the following criteria:

- Syslog message ID number
- Syslog message severity level
- Syslog message class (equivalent to a functional area of the adaptive security appliance)

You customize these criteria by creating a message list that you can specify when you set the output destination. Alternatively, you can configure the adaptive security appliance to send a particular message class to each type of output destination independently of the message list.

You can use syslog message classes in two ways:

- Specify an output location for an entire category of syslog messages using the **logging class** command.
- Create a message list that specifies the message class using the **logging list** command.

The syslog message class provides a method of categorizing syslog messages by type, equivalent to a feature or function of the adaptive security appliance. For example, the vpnc class denotes the VPN client.

All syslog messages in a particular class share the same initial three digits in their syslog message ID numbers. For example, all syslog message IDs that begin with the digits 611 are associated with the vpnc (VPN client) class. Syslog messages associated with the VPN client feature range from 611101 to 611323.

In addition, most of the ISAKMP syslog messages have a common set of prepended objects to help identify the tunnel. These objects precede the descriptive text of a syslog message when available. If the object is not known at the time the syslog message is generated, the specific *heading* = *value* combination is not displayed.

The objects are prefixed as follows:

Group = *groupname*, Username = *user*, IP = *IP_address*, ...

Where the group identifies the tunnel-group, the username is the username from the local database or AAA server, and the IP address is the public IP address of the remote access client or L2L peer.

Using Custom Message Lists

Creating a custom message list is a flexible way to exercise control over which syslog messages are sent to which output destination. In a custom syslog message list, you specify groups of syslog messages using any or all of the following criteria: severity level, message IDs, ranges of syslog message IDs, or message class.

For example, you can use message lists to do the following:

- Select syslog messages with severity levels of 1 and 2 and send them to one or more e-mail addresses.
- Select all syslog messages associated with a message class (such as ha) and save them to the internal buffer.

A message list can include multiple criteria for selecting messages. However, you must add each message selection criterion with a new command entry. It is possible to create a message list that includes overlapping message selection criteria. If two criteria in a message list select the same message, the message is logged only once.

Licensing Requirements for Logging

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Prerequisites for Logging

Logging has the following prerequisites:

- The syslog server must run a server program called syslogd. Windows (except for Windows 95 and Windows 98) provides a syslog server as part of its operating system. For Windows 95 and Windows 98, you must obtain a syslogd server from another vendor.
- To view logs generated by the adaptive security appliance, you must specify a logging output destination. If you enable logging without specifying a logging output destination, the adaptive security appliance generates messages but does not save them to a location from which you can view them. You must specify each different logging output destination separately. For example, to designate more than one syslog server as an output destination, enter a new command for each syslog server.

Guidelines and Limitations

Context Mode Guidelines

Supported in single and multiple context modes.

Firewall Mode Guidelines

Supported in routed and transparent firewall modes.

IPv6 Guidelines

Supports IPv6.

Additional Guidelines

Sending syslogs over TCP is not supported on a standby adaptive security appliance.

Configuring Logging

This section describes how to configure logging, and includes the following topics:

- Enabling Logging, page 72-6
- Configuring an Output Destination, page 72-6

Note The minimum configuration depends on what you want to do and what your requirements are for handling syslog messages in the adaptive security appliance.

Enabling Logging

To enable logging, enter the following command:

Command	Purpose

`logging enable`
 	
Example:
`hostname(config)# logging enable`
	Enables logging. To disable logging, enter the **no logging enable** command.

What to Do Next

See the "Configuring an Output Destination" section on page 72-6.

Configuring an Output Destination

To optimize syslog message usage for troubleshooting and performance monitoring, we recommend that you specify one or more locations where syslog messages should be sent, including an internal log buffer, one or more external syslog servers, ASDM, an SNMP management station, the console port, specified e-mail addresses, or Telnet and SSH sessions.

This section includes the following topics:

- Sending Syslog Messages to an External Syslog Server, page 72-8
- Sending Syslog Messages to the Internal Log Buffer, page 72-9
- Sending Syslog Messages to an E-mail Address, page 72-10
- Sending Syslog Messages to ASDM, page 72-11
- Sending Syslog Messages to the Console Port, page 72-11

- Sending Syslog Messages to an SNMP Server, page 72-12
- Sending Syslog Messages to a Telnet or SSH Session, page 72-12
- Creating a Custom Event List, page 72-13
- Generating Syslog Messages in EMBLEM Format to a Syslog Server, page 72-14
- Generating Syslog Messages in EMBLEM Format to Other Output Destinations, page 72-14
- Changing the Amount of Internal Flash Memory Available for Logs, page 72-14
- Sending All Syslog Messages in a Class to a Specified Output Destination, page 72-15
- Enabling Secure Logging, page 72-16
- Including the Device ID in Non-EMBLEM Format Syslog Messages, page 72-17
- Including the Date and Time in Syslog Messages, page 72-18
- Disabling a Syslog Message, page 72-18
- Changing the Severity Level of a Syslog Message, page 72-18
- Limiting the Rate of Syslog Message Generation, page 72-19

Sending Syslog Messages to an External Syslog Server

You can archive messages according to the available disk space on the external syslog server, and manipulate logging data after it is saved. For example, you could specify actions to be executed when certain types of syslog messages are logged, extract data from the log and save the records to another file for reporting, or track statistics using a site-specific script.

To send syslog messages to an external syslog server, perform the following steps:

	Command	Purpose
Step 1	**logging host** *interface_name syslog_ip* [**tcp**[*/port*] | **udp**[*/port*] [**format emblem**]] **Example:** `hostname(config)# logging host dmz1 192.168.1.5 udp 1026 format emblem`	Configures the adaptive security appliance to send messages to a syslog server. The **format emblem** keyword enables EMBLEM format logging for the syslog server (UDP only). The *interface_name* argument specifies the interface through which you access the syslog server. The *syslog_ip* argument specifies the IP address of the syslog server. The **tcp**[**/***port*] or **udp**[**/***port*] argument specifies that the adaptive security appliance should use TCP or UDP to send syslog messages to the syslog server. You can configure the adaptive security appliance to send data to a syslog server using either UDP or TCP, but not both. The default protocol is UDP if you do not specify a protocol. If you specify TCP, the adaptive security appliance discovers when the syslog server fails and as a security protection, new connections through the adaptive security appliance are blocked. To allow new connections regardless of connectivity to a TCP syslog server, see Step 3. If you specify UDP, the adaptive security appliance continues to allow new connections whether or not the syslog server is operational. Valid port values for either protocol are 1025 through 65535. The default UDP port is 514. The default TCP port is 1470. **Note** Sending syslogs over TCP is not supported on a standby adaptive security appliance.
Step 2	**logging trap** {*severity_level* | *message_list*} **Example:** `hostname(config)# logging trap errors`	Specifies which syslog messages should be sent to the syslog server. You can specify the severity level number (1 through 7) or name. For example, if you set the severity level to 3, then the adaptive security appliance sends syslog messages for severity levels 3, 2, and 1. You can specify a custom message list that identifies the syslog messages to send to the syslog server.

	Command	Purpose
Step 3	**logging permit-hostdown** **Example:** `hostname(config)# logging permit-hostdown`	(Optional) Disables the feature to block new connections when a TCP-connected syslog server is down. If the adaptive security appliance is configured to send syslog messages to a TCP-based syslog server, and if either the syslog server is down or the log queue is full, then new connections are blocked. New connections are allowed again after the syslog server is back up and the log queue is no longer full. For more information about the log queue, see the "Configuring the Logging Queue" section on page 72-15.
Step 4	**logging facility** number **Example:** `hostname(config)# logging facility 21`	(Optional) Sets the logging facility to a value other than 20, which is what most UNIX systems expect.

Sending Syslog Messages to the Internal Log Buffer

To send syslog messages to the internal log buffer, perform the following steps:

	Command	Purpose

Step 1	**logging buffered** {*severity_level* | *message_list*}
	
	Example:
	`hostname(config)# logging buffered critical`
	
	`hostname(config)# logging buffered level 2`
	
	`hostname(config)# logging buffered notif-list`
		Specifies which syslog messages should be sent to the internal log buffer, which serves as a temporary storage location. New messages are appended to the end of the list. When the buffer is full, that is, when the buffer wraps, old messages are overwritten as new messages are generated, unless you configure the adaptive security appliance to save the full buffer to another location. To empty the internal log buffer, enter the **clear logging buffer** command.

Step 2	**logging buffer-size** *bytes* **Example:** `hostname(config)# logging buffer-size 16384`	Changes the size of the internal log buffer. The buffer size is 4 KB.
Step 3	Choose one of the following options:	
	logging flash-bufferwrap **Example:** `hostname(config)# logging flash-bufferwrap`	When saving the buffer content to another location, the adaptive security appliance creates log files with names that use the following time-stamp format: *LOG-YYYY-MM-DD-HHMMSS.TXT* where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds. The adaptive security appliance continues to save new messages to the internal log buffer and saves the full log buffer content to the internal flash memory.

Command	Purpose
logging ftp-bufferwrap **Example:** `hostname(config)# logging ftp-bufferwrap`	When saving the buffer content to another location, the adaptive security appliance creates log files with names that use the following time-stamp format: *LOG-YYYY-MM-DD-HHMMSS.TXT* where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds. The adaptive security appliance continues saving new messages to the internal log buffer and saves the full log buffer content to an FTP server.
logging ftp-server *server path username password* **Example:** `hostname(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs`	Identifies the FTP server on which you want to store log buffer content. The *server* argument specifies the IP address of the external FTP server. The *path* argument specifies the directory path on the FTP server where the log buffer data is to be saved. This path is relative to the FTP root directory. The *username* argument specifies a username that is valid for logging into the FTP server. The *password* argument indicates the password for the username specified.
logging savelog [*savefile*] **Example:** `hostname(config)# logging savelog latest-logfile.txt`	Saves the current log buffer content to the internal flash memory.

Sending Syslog Messages to an E-mail Address

To send syslog messages to an e-mail address, perform the following steps:

	Command	Purpose
Step 1	**logging mail** {severity_level | message_list} **Example:** `hostname(config)# logging mail high-priority`	Specifies which syslog messages should be sent to an e-mail address. When sent by e-mail, a syslog message appears in the subject line of the e-mail message. For this reason, we recommend configuring this option to notify administrators of syslog messages with high severity levels, such as critical, alert, and emergency.
Step 2	**logging from-address** *email_address* **Example:** `hostname(config)# logging from-address xxx-001@example.com`	Specifies the source e-mail address to be used when sending syslog messages to an e-mail address.

	Command	Purpose
Step 3	**logging recipient-address** *e-mail_address [severity_level]* **Example:** `hostname(config)# logging recipient-address admin@example.com`	Specifies the recipient e-mail address to be used when sending syslog messages to an e-mail address.
Step 4	**smtp-server** *ip_address* **Example:** `hostname(config)# smtp-server 10.1.1.1`	Specifies the SMTP server to be used when sending syslog messages to an e-mail address.

Sending Syslog Messages to ASDM

To send syslog messages to ASDM, perform the following steps:

	Command	Purpose
Step 1	**logging asdm** {*severity_level* | *message_list*} **Example:** `hostname(config)# logging asdm 2`	Specifies which syslog messages should be sent to ASDM. The adaptive security appliance sets aside a buffer area for syslog messages waiting to be sent to ASDM and saves messages in the buffer as they occur. The ASDM log buffer is a different buffer than the internal log buffer. When the ASDM log buffer is full, the adaptive security appliance deletes the oldest syslog message to make room in the buffer for new ones. This is the default setting in ASDM. To control the number of syslog messages retained in the ASDM log buffer, you can change the size of the buffer.
Step 2	**logging asdm-buffer-size** *num_of_msgs* **Example:** `hostname(config)# logging asdm-buffer-size 200`	Specifies the number of syslog messages to be retained in the ASDM log buffer. To empty the current content of the ASDM log buffer, enter the **clear logging asdm** command.

Sending Syslog Messages to the Console Port

To send syslog messages to the console port, perform the following steps:

Command	Purpose
logging console {severity_level | message_list} **Example:** `hostname(config)# logging console errors`	Specifies which syslog messages should be sent to the console port.

Sending Syslog Messages to an SNMP Server

To enable logging to an SNMP server, perform the following steps:

Command	Purpose
logging history [*logging_list* | *level*] **Example:** `hostname(config)# logging history errors`	Enables SNMP logging and specifies which messages are to be sent to SNMP servers. To disable SNMP logging, enter the **no logging history** command.

Sending Syslog Messages to a Telnet or SSH Session

To send syslog messages to a Telnet or SSH session, perform the following steps:

	Command	Purpose
Step 1	**logging monitor** {*severity_level* | *message_list*} **Example:** `hostname(config)# logging monitor 6`	Specifies which syslog messages should be sent to a Telnet or SSH session.
Step 2	**terminal monitor** **Example:** `hostname(config)# terminal monitor`	Enables logging to the current session only. If you log out and then log in again, you need to reenter this command. To disable logging to the current session, enter the **terminal no monitor** command.

Creating a Custom Event List

To create a custom event list, perform the following steps:

	Command	Purpose
Step 1	**logging list** *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]} **Example:** `hostname(config)# logging list notif-list level 3`	Specifies criteria for selecting messages to be saved in the internal log buffer. For example, if you set the severity level to 3, then the adaptive security appliance sends syslog messages for severity levels 3, 2, and 1. The *name* argument specifies the name of the list. The **level** *level* argument specifies the severity level. The **class** *message_class* argument specifies a particular message class. The **message** *start_id*[**-***end_id*] argument specifies an individual syslog message number or a range of numbers. **Note** Do not use the names of severity levels as the name of a syslog message list. Prohibited names include emergencies, alert, critical, error, warning, notification, informational, and debugging. Similarly, do not use the first three characters of these words at the beginning of an event list name. For example, do not use an event list name that starts with the characters err.

Step 2	**logging list** *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}
	
	Example:
	`hostname(config)# logging list notif-list 104024-105999`
	
	`hostname(config)# logging list notif-list level critical`
	
	`hostname(config)# logging list notif-list level warning class ha`
		(Optional) Adds more criteria for message selection to the list. Enter the same command as in the previous step, specifying the name of the existing message list and the additional criterion. Enter a new command for each criterion that you want to add to the list. For example, you can specify criteria for syslog messages to be included in the list as the following:
		
		• Syslog message IDs that fall into the range of 104024 to 105999.
		• All syslog messages with the critical severity level or higher (emergency, alert, or critical).
		• All ha class syslog messages with the warning severity level or higher (emergency, alert, critical, error, or warning).
		
		Note A syslog message is logged if it satisfies any of these conditions. If a syslog message satisfies more than one of the conditions, the message is logged only once.

Generating Syslog Messages in EMBLEM Format to a Syslog Server

To generate syslog messages in EMBLEM format to a syslog server, perform the following steps:

Command	Purpose
logging host *interface_name ip_address* {**tcp**[*/port*] | **udp**[*/port*]} [**format emblem**] **Example:** `hostname(config)# logging host interface_1 127.0.0.1 udp format emblem`	Sends syslog messages in EMBLEM format to a syslog server over UDP using port 514.

Generating Syslog Messages in EMBLEM Format to Other Output Destinations

To generate syslog messages in EMBLEM format to other output destinations, perform the following steps:

Command	Purpose
logging emblem **Example:** `hostname(config)# logging emblem`	Sends syslog messages in EMBLEM format to output destinations other than a syslog server, such as Telnet or SSH sessions.

Changing the Amount of Internal Flash Memory Available for Logs

To change the amount of internal flash memory available for logs, perform the following steps:

	Command	Purpose
Step 1	**logging flash-maximum-allocation** *kbytes* **Example:** `hostname(config)# logging flash-maximum-allocation 1200`	Specifies the maximum amount of internal flash memory available for saving log files. By default, the adaptive security appliance can use up to 1 MB of internal flash memory for log data. The minimum amount of internal flash memory that must be free for the adaptive security appliance to save log data is 3 MB. If a log file being saved to internal flash memory would cause the amount of free internal flash memory to fall below the configured minimum limit, the adaptive security appliance deletes the oldest log files to ensure that the minimum amount of memory remains free after saving the new log file. If there are no files to delete or if, after all old files have been deleted, free memory is still below the limit, the adaptive security appliance fails to save the new log file.
Step 2	**logging flash-minimum-free** *kbytes* **Example:** `hostname(config)# logging flash-minimum-free 4000`	Specifies the minimum amount of internal flash memory that must be free for the adaptive security appliance to save a log file.

Configuring the Logging Queue

To configure the logging queue, perform the following steps:

Command	Purpose
logging queue *message_count* **Example:** `hostname(config)# logging queue 300`	Specifies the number of syslog messages that the adaptive security appliance can hold in its queue before sending them to the configured output destination. The adaptive security appliance has a fixed number of blocks in memory that can be allocated for buffering syslog messages while they are waiting to be sent to the configured output destination. The number of blocks required depends on the length of the syslog message queue and the number of syslog servers specified. The default queue size is 512 syslog messages. The queue size is limited only by block memory availability. Valid values are from 0 to 8192 messages, depending on the platform. If the logging queue is set to zero, the queue will be the maximum configurable size (8192 messages), depending on the platform. The maximum queue size by platform is as follows: • ASA-5505—1024 • ASA-5510—2048 • On all other platforms—8192

Sending All Syslog Messages in a Class to a Specified Output Destination

To send all syslog messages in a class to a specified output destination, perform the following steps:

Command	Purpose
logging class *message_class* {**buffered** | **console** | **history** | **mail** | **monitor** | **trap**} [*severity_level*] **Example:** `hostname(config)# logging class ha buffered alerts`	Overrides the configuration in the specified output destination command. For example, if you specify that messages at severity level 7 should go to the internal log buffer and that ha class messages at severity level 3 should go to the internal log buffer, then the latter configuration takes precedence. The **buffered**, **history**, **mail**, **monitor**, and **trap** keywords specify the output destination to which syslog messages in this class should be sent. The **history** keyword enables SNMP logging. The **monitor** keyword enables Telnet and SSH logging. The **trap** keyword enables syslog server logging. Select one destination per command line entry. To specify that a class should go to more than one destination, enter a new command for each output destination.

Enabling Secure Logging

To enable secure logging, perform the following steps:

Command	Purpose
logging host *interface_name syslog_ip* [**tcp**/port | **udp**/*port*] [**format emblem**] [**secure**] **Example:** `hostname(config)# logging host inside 10.0.0.1 TCP/1500 secure`	Enables secure logging. The *interface_name* argument specifies the interface on which the syslog server resides. The *syslog_ip* argument specifies the IP address of the syslog server. The *port* argument specifies the port (TCP or UDP) that the syslog server listens to for syslog messages. The **tcp** keyword specifies that the adaptive security appliance should use TCP to send syslog messages to the syslog server. The **udp** keyword specifies that the adaptive security appliance should use UDP to send syslog messages to the syslog server. The **format emblem** keyword enables EMBLEM format logging for the syslog server. The **secure** keyword specifies that the connection to the remote logging host should use SSL/TLS for TCP only. Secure logging does not support UDP; an error occurs if you try to use this protocol.

Including the Device ID in Non-EMBLEM Format Syslog Messages

To include the device ID in non-EMBLEM format syslog messages, perform the following steps:

Command	Purpose

logging device-id [**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*]
 	
Example:
`hostname(config)# logging device-id hostname`
 	
`hostname(config)# logging device-id context-name`
	Configures the adaptive security appliance to include a device ID in non-EMBLEM-format syslog messages. You can specify only one type of device ID for syslog messages.The **context-name** keyword indicates that the name of the current context should be used as the device ID (applies to multiple context mode only). If you enable the logging device ID for the admin context in multiple context mode, messages that originate in the system execution space use a device ID of **system**, and messages that originate in the admin context use the name of the admin context as the device ID.
	
	The **hostname** keyword specifies that the hostname of the adaptive security appliance should be used as the device ID. The **ipaddress** *interface_name* argument specifies that the IP address of the interface specified as *interface_name* should be used as the device ID. If you use the **ipaddress** keyword, the device ID becomes the specified adaptive security appliance interface IP address, regardless of the interface from which the syslog message is sent. This keyword provides a single, consistent device ID for all syslog messages that are sent from the device. The **string** *text* keyword and argument specify that the text string should be used as the device ID. The string can include as many as 16 characters. You cannot use blank spaces or any of the following characters:
	• & (ampersand)
	• ‘ (single quote)
	• “ (double quote)
	• < (less than)
	• > (greater than)
	• ? (question mark)
	
	Note If enabled, the device ID does not appear in EMBLEM-formatted syslog messages nor in SNMP traps.

Including the Date and Time in Syslog Messages

To include the date and time in syslog messages, perform the following steps:

Command	Purpose

logging timestamp
`hostname(config)# logging timestamp`
 	
Example:
`hostname(config)# logging timestamp`
`LOG-2008-10-24-081856.TXT`
	Specifies that syslog messages should include the date and time that they were generated. To remove the date and time from syslog messages, enter the **no logging timestamp** command.

Disabling a Syslog Message

To disable a specified syslog message, perform the following steps:

Command	Purpose
no logging message *message_number* **Example:** `hostname(config)# no logging message 113019`	Prevents the adaptive security appliance from generating a particular syslog message. To reenable a disabled syslog message, enter the **logging message** *message_number* command (for example, **logging message 113019**). To reenable logging of all disabled syslog messages, enter the **clear config logging disabled** command.

Changing the Severity Level of a Syslog Message

To change the severity level of a syslog message, perform the following steps:

Command	Purpose
logging message *message_ID* **level** *severity_level* **Example:** `hostname(config)# logging message 113019 level 5`	Specifies the severity level of a syslog message. To reset the severity level of a syslog message to its setting, enter the **no logging message** *message_ID* **level** *current_severity_level* command (for example, **no logging message 113019 level 5**). To reset the severity level of all modified syslog messages to their settings, enter the **clear configure logging level** command.

Limiting the Rate of Syslog Message Generation

To limit the rate of syslog message generation, perform the following steps:

Command	Purpose
logging rate-limit {unlimited | {*num* [*interval*]}} message *syslog_id* | level *severity_level* **Example:** hostname(config)# logging rate-limit 1000 600 level 6	Applies a specified severity level (1 through 7) to a set of messages or to an individual message (not the destination) within a specified time period. Rate limits affect the volume of messages being sent to all configured destinations. To reset the logging rate-limit to the value, enter the **clear running-config logging rate-limit** command. To reset the logging rate-limit, enter the **clear configure logging rate-limit** command.

Log Monitoring

To perform log monitoring and assist in monitoring system performance, enter the following command:

Command	Purpose
show logging	Shows syslog messages, including the severity level. **Note** The maximum number of syslog messages that are available to view is 1000, which is the default setting. The maximum number of syslog messages that are available to view is 2000.
show logging message	Shows a list of syslog messages with modified severity levels and disabled syslog messages.
show logging message *message_ID*	Shows the severity level of a specific syslog message.
show logging queue	Shows the logging queue and queue statistics.
show logging rate-limit	Shows the disallowed syslog messages.
show running-config logging rate-limit	Shows the current logging rate-limit setting.

Examples

The following example shows the logging information that displays for the **show logging** command:

```
hostname(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
```

```
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

Configuration Examples for Logging

The following examples show how to control both whether a syslog message is enabled and the severity level of the specified syslog message:

```
hostname(config)# show logging message 403503
syslog 403503: -level errors (enabled)

hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: -level errors (enabled)
```

Feature History for Logging

Table 72-2 lists each feature change and the platform release in which it was implemented.

Table 72-2 Feature History for Logging

Feature Name	Platform Releases	Feature Information
Logging	7.0(1)	Provides adaptive security appliance network logging information through various output destinations, and includes the option to view and save log files.
Rate limit	7.0(4)	Limits the rate at which syslog messages are generated. The **logging rate-limit** command was introduced.
Logging list	7.2(1)	Creates a logging list to use in other commands to specify messages by various criteria (logging level, event class, and message IDs). The **logging list** command was introduced.

Table 72-2 Feature History for Logging (continued)

Feature Name	Platform Releases	Feature Information
Secure logging	8.0(2)	Specifies that the connection to the remote logging host should use SSL/TLS. This option is valid only if the protocol selected is TCP. The **logging host** command was modified.
Logging class	8.0(4), 8.1(1)	Added support for the ipaa event class of logging messages. The **logging class** command was modified.
Logging class and saved logging buffers	8.2(1)	Added support for the dap event class of logging messages. The **logging class** command was modified. Added support to clear the saved logging buffers (ASDM, internal, FTP, and flash). The **clear logging queue bufferwrap** command was introduced.
Password encryption	8.3(1)	Added support for password encryption. The **logging ftp server command** was modified.
Enhanced logging and connection blocking	8.3(2)	When you configure a syslog server to use TCP, and the syslog server is unavailable, the adaptive security appliance blocks new connections that generate syslog messages until the server becomes available again (for example, VPN, firewall, and cut-through-proxy connections). This feature has been enhanced to also block new connections when the logging queue on the adaptive security appliance is full; connections resume when the logging queue is cleared. This feature was added for compliance with Common Criteria EAL4+. Unless required, we recommended allowing connections when syslog messages cannot be sent or received. To allow connections, continue to use the **logging permit-hostdown** command. The following command was modified: **show logging**. The following syslog messages were introduced: 414005, 414006, 414007, and 414008.